

(12) 发明专利

(10) 授权公告号 CN 1868162 B

(45) 授权公告日 2012.10.03

(21) 申请号 200480030203.X

(51) Int. Cl.

(22) 申请日 2004.09.02

H04L 9/08(2006.01)

(30) 优先权数据

60/499,563 2003.09.02 US

60/502,866 2003.09.11 US

10/932,514 2004.09.01 US

(85) PCT申请进入国家阶段日

2006.04.14

(56) 对比文件

US 2003/0030581 A1, 2003.02.13, 说明书第60-91段.

US 5371794 A, 1994.12.06, 摘要、说明书第7栏第63行-第8栏倒数第1行, 第10栏第24-56行, 图5a, 5b.

CN 1427575 A, 2003.07.02, 全文.

审查员 高静

(86) PCT申请的申请数据

PCT/US2004/028677 2004.09.02

(87) PCT申请的公布数据

W02005/029762 EN 2005.03.31

(73) 专利权人 高通股份有限公司

地址 美国加利福尼亚州

(72) 发明人 J·森普尔 G·G·罗斯

(74) 专利代理机构 北京市柳沈律师事务所

11105

代理人 邵亚丽

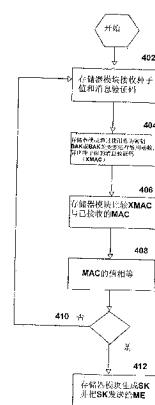
权利要求书 3 页 说明书 8 页 附图 8 页

(54) 发明名称

向通信系统中的广播多播通信提供已验证询问的方法和设备

(57) 摘要

本发明公开了在多播-广播-多媒体系统中安全生成用于观看信息内容的短期密钥 SK 的方法和设备。只有当用来生成短期密钥的信息源可以被验证时,位于用户设备 (UE) 的存储器模块生成短期密钥。短期密钥可以由广播接入密钥 (NAK) 或 BAK 的变型和附有消息验证码 (MAC) 的变化值生成。还可以通过使用私有密钥,以及短期密钥 (SK) 管理器使用数字签名把相应的公用密钥分配给设置在用户设备 (UE) 中的存储器,来生成短期密钥 (SK)。



1. 一种在用于对移动台进行点对多点内容传输的通信系统中,安全地获得用于使用移动台访问内容的短期密钥的方法,包括 :

从用于对移动台进行点对多点内容传输的通信系统中的短期密钥管理器接收第一值和第一消息验证码 ;

通过使用接收移动台的安全存储器中存储的共享秘密密钥对已接收的第一值运行散列函数,生成作为第一值的函数的第二消息验证码 ;其中,所述共享秘密密钥由预定点对多点传输的每个移动台安全的存储,并且,其中所述安全存储器中存储的共享秘密密钥对于所述接收移动台的移动设备是受到保护的 ;

比较所述第二消息验证码与已接收的第一消息验证码 ;和

如果所述第二消息验证码等于所述第一消息验证码,使用所述第一值和共享秘密密钥算出短期密钥,其中所述移动设备使用短期密钥访问所述内容。

2. 根据权利要求 1 所述的方法,其中所述第一值由短期密钥管理器确定。

3. 根据权利要求 1 所述的方法,其中所述第一值包括时间戳。

4. 根据权利要求 1 所述的方法,其中用于生成第二消息验证码的散列函数包括安全散列算法 1(SHA-1) 和 Rivest 散列函数 MD-5 之一。

5. 根据权利要求 1 所述的方法,还包括把来自安全存储器的已计算的短期密钥发送给移动设备。

6. 一种在用于对移动台进行点对多点内容传输的通信系统中安全地获得用于使用移动台访问内容的短期密钥的方法,所述方法包括以下步骤 :

从用于对移动台进行点对多点内容传输的通信系统中的短期密钥管理器接收第一值和由私有密钥形成的第一数字签名 ;

使用对所述私有密钥的签名方案和公共密钥,验证所述第一数字签名,其中所述公共密钥被存储在接收移动台的第一安全存储器中,并且签名方案被存储在第一安全存储器中,并且,其中所述安全存储器中存储的公共密钥对于所述接收移动台的移动设备是受到保护的 ;

确定所述第一数字签名的源是短期密钥管理器 ;和

如果所述第一数字签名被确定为由短期密钥管理器生成,则使用所述第一值和公共密钥算出短期密钥,其中所述移动设备使用短期密钥访问所述内容。

7. 一种利用第一协议在用于对移动台进行点对多点内容传输的通信系统中获得加密密钥的方法,所述方法包括以下步骤 :

从用于对移动台进行点对多点内容传输的通信系统中的分组索引管理器接收分组索引值和第一消息验证码 ;

通过使用接收移动台的安全存储器中存储的共享秘密密钥对分组索引值运行散列函数,利用分组索引值生成第二消息验证码,其中,所述共享秘密密钥由预定点对多点传输的每个移动台安全的存储,并且,其中所述安全存储器中存储的共享秘密密钥对于所述接收移动台的移动设备是受到保护的 ;

将所述第二消息验证码与所述第一消息验证码进行比较 ;和

如果所述第二消息验证码等于所述第一消息验证码,则利用所述分组索引值和所述共享秘密密钥算出加密密钥,其中所述移动设备使用加密密钥访问所述内容。

8. 根据权利要求 7 所述的方法, 其中所述第一协议是安全实时传输协议 (SRTP)。
9. 根据权利要求 7 所述的方法, 其中所述分组索引值包括序号。
10. 根据权利要求 7 所述的方法, 其中所述共享秘密密钥包括主密钥。
11. 根据权利要求 7 所述的方法, 其中用于生成第二消息验证码的散列函数包括安全散列算法 1(SHA-1) 和 Rivest 散列函数 MD-5 之一。
12. 根据权利要求 7 所述的方法, 还包括把所述加密密钥发送给移动设备。

13. 一种利用第一协议在用于对移动台进行点对多点内容传输的通信系统中获得加密密钥的方法, 所述方法包括以下步骤 :

从用于对移动台进行点对多点内容传输的通信系统中的分组索引管理器接收分组索引值和由私有密钥形成的第一数字签名 ;

使用对私有密钥的签名方案和公共密钥, 验证第一数字签名, 其中所述公共密钥被存储在接收移动台的第一安全存储器中, 所述签名方案被存储在所述第一安全存储器中, 并且, 其中所述安全存储器中存储的公共密钥对于所述接收移动台的移动设备是受到保护的 ;

确定所述数字签名的源是所述分组索引管理器 ; 和

如果所述第一数字签名被确定为由所述分组索引管理器生成, 则使用所述分组索引值和所述公共密钥算出加密密钥, 其中所述移动设备使用所述加密密钥访问所述内容。

14. 一种在用于对移动台进行点对多点内容传输的通信系统中安全地获得短期密钥的移动台设备, 包括 :

用于从对移动台进行点对多点内容传输的通信系统中的短期密钥管理器接收第一值和第一消息验证码的装置 ;

用于通过使用移动台设备的安全存储器中存储的共享秘密密钥对第一值运行散列函数, 生成作为第一值的函数的第二消息验证码的装置, 其中, 所述共享秘密密钥由预定点对多点传输的每个移动台安全的存储, 并且, 其中所述安全存储器中存储的共享秘密密钥对于所述移动台设备的移动设备是受到保护的 ;

用于比较所述第二消息验证码与所述第一消息验证码的装置 ; 和

用于如果所述第二消息验证码等于所述第一消息验证码, 则使用所述第一值和所述共享秘密密钥算出短期密钥的装置。

15. 根据权利要求 14 所述的设备, 其中所述第一值包括时间戳。

16. 根据权利要求 14 所述的设备, 其中散列函数包括安全散列算法 1(SHA-1) 和 Rivest 散列函数 MD-5 之一。

17. 根据权利要求 14 所述的设备, 还包括用于把来自安全存储器的算出的短期密钥发送给所述移动台设备的移动设备。

18. 一种利用第一协议获得加密密钥的移动台设备, 包括 :

用于从通信系统中的分组索引管理器接收分组索引值和第一消息验证码的装置, 其中所述通信系统用于对移动台进行点对多点内容传输 ;

用于通过使用共享秘密密钥对分组索引值运行散列函数, 生成分组索引值的第二消息验证码的装置, 其中, 所述共享秘密密钥被存储在所述移动台设备的安全存储器中, 其中, 所述共享秘密密钥由预定点对多点传输的每个移动台安全的存储, 并且, 其中所述安全存

储器中存储的共享秘密密钥相对所述移动台设备的移动设备是受到保护的；

用于将所述第二消息验证码与所述第一消息验证码进行比较的装置；和

用于如果第二消息验证码等于第一消息验证码，则利用分组索引值和共享秘密密钥算出加密密钥的装置，其中所述移动设备使用加密密钥访问所述内容。

19. 根据权利要求 18 所述的设备，其中所述第一协议是安全实时传输协议 (SRTP)。

20. 根据权利要求 18 所述的设备，其中所述分组索引值包括随机数。

21. 根据权利要求 18 所述的设备，其中散列函数包括安全散列算法 1 (SHA-1) 和 Rivest 散列函数 MD-5 之一。

22. 根据权利要求 18 所述的设备，其中所述共享秘密密钥是主密钥。

23. 根据权利要求 18 所述的设备，还包括把所述加密密钥发送给移动设备。

向通信系统中的广播多播通信提供已验证询问的方法和设备

[0001] 按照 35U. S. C. § 119 要求的优先权

[0002] 本申请要求 2003 年 9 月 2 日提交的 60/499,563 号美国临时申请和 2003 年 9 月 11 日提交的 60/502,866 号美国临时申请的优先权，它们二者可被转让给其受让人，从而可将其明确引用在此作为参考。

技术领域

[0003] 本发明总体涉及通信，特别涉及向无线通信系统中的广播多播服务 (BCMCS) 提供已验证询问的方法和设备。

背景技术

[0004] 在传输非语音业务如视频、数据、多媒体或除语音业务之外的其它类型业务的无线通信系统中，典型的蜂窝基站可以向基站覆盖区域内的多个移动台广播多媒体业务服务。多媒体业务服务可以包括任何数量的信息服务，例如类似于有线电视服务规划中包含的多个通道。这些信息服务通常依赖于支持责任性、公证性、精确性、机密性和可操作性的安全性。加密或者密码技术的普通字段用于电子商务、无线通信和广播。在电子商务中，加密用来防止欺诈并用来检验金融交易。在数据处理系统中，加密用来检验参与者的身份。在广播多播服务中，根据广播多播服务 (BCMCS) 密钥层级保持安全性。内容用短期密钥 (SK) 加密并无线发送。长期加密密钥经常称作广播接入密钥 (BAK)，它被设置到称作移动台的用户标识模块 (UIM) 或者通用集成电路卡 (UICC) 的存储器模块中。可以向用户收取长期加密密钥 BAK 的费用。短期密钥 SK 源自 BAK 和称之为 SKEAND 的随机数。UIM 使用 BAK 和 SKRAND 计算短期密钥 SK。一旦 UIM 计算 SK，就把它发送给移动台，于是移动台使用 SK 解密并观看信息内容。通常，一旦收到 BAK，就像用户收取基于该方法计费的信息内容的费用。因此无论用户实际上是否观看了该广播内容，都要被收费。与有线电视不同，在无线通信系统中，人们希望保持用户的信息服务的实际观看时间。这确保了所看内容的精确记帐，并保证未授权用户如未成年用户例如不能访问某些类型的内容。需要移动台周期地注册或者在要求时注册的方法已经被提出，以便保持用户的实际观看时间的记录。注册消息包含用户正在观看或者能够观看的信道列表。该列表用来向用户收取信息服务的费用。

[0005] 通常，需要用户周期注册或者在要求时注册的方法容易出现服务偷窃，因为移动台可以连续接收广播内容而不需在系统上再次注册，从而获得对内容的免费访问。此外，例如，未授权用户如未成年用户可以访问被管理法禁止的内容。其它的建议方法引入了观看信息服务内容必需的附加的加密密钥。这些方法遭受到无线系统的数据承载能力的严重降低，这是加密密钥管理所需的开销消息的增加造成的。

发明内容

[0006] 本发明的目的是克服或者至少降低上述一个或多个问题的影响。

[0007] 根据一个方面，在无线通信系统中，为广播多播业务提供已验证询问的一种方法，包括：接收第一值和第一消息验证码；通过使用第二值对第一值运行散列(hashing)函数，生成第一值的第二消息验证码，其中第二值作为第二密钥被存储在存储器模块中；比较第二消息验证码与第一消息验证码；当第二消息验证码等于第一消息验证码时，使用第一值和第二值计算短期密钥。

[0008] 在另一个方面，提供了一种使用第一协议获得通信系统中加密密钥的方法，该方法包括：接收分组索引值和第一消息验证码；通过使用第二值对分组索引值运行散列函数，生成分组索引值的第二消息验证码，其中第二值被存储在存储器模块中；比较第二消息验证码与第一消息验证码；当第二消息验证码等于第一消息验证码时，使用分组索引值和第二值计算加密密钥。

[0009] 在另一方面，提供了一种获得短期密钥的移动台设备，包括：接收第一值和第一消息验证码的装置；通过使用第二值对第一值运行散列函数，生成第一值的第二消息验证码的装置，其中第二值被存储在存储器模块中；比较第二消息验证码与第一消息验证码的装置；当第二消息验证码等于第一消息验证码时，使用第一值和第二值计算短期密钥的装置。

[0010] 在另一个方面，提供了一种使用第一协议获得加密密钥的移动台设备，包括：接收分组索引值和第一消息验证码的装置；通过使用第二值对分组索引值运行散列函数，生成分组索引值的第二消息验证码的装置，其中第二值被存储在存储器模块中；比较第二消息验证码与第一消息验证码的装置；当生成的消息验证码等于接收的消息验证码时，使用分组索引值和第二值计算加密密钥。

附图说明

[0011] 图1是图示本发明实施例的提供广播多播通信服务(BCMCS)的无线通信系统的示范实施例；

[0012] 图2是本发明一个实施例的使用随机数在用户设备中生成短期密钥(SK)的示范方框图；

[0013] 图3是本发明实施例的使用具有附加在其上的消息验证码的种子值(SKSeed)在用户设备中生成短期密钥(SK)的示范方框图；

[0014] 图4是本发明一个实施例的使用具有附加到其上的消息验证码的种子值(SKSeed)生成短期密钥(SK)的示范流程图；

[0015] 图5是本发明的一个实施例的用具有私有密钥的SK管理器生成短期密钥(SK)的示范方框图，其中相应的公用密钥被分配给用户设备；

[0016] 图6是本发明一个实施例的使用具有附加到其上的消息验证码的分组索引种子值(PISeed)，在用户设备中生成加密密钥(EK)的示范方框图；

[0017] 图7是本发明一个实施例的使用具有附加到其上的消息验证码的分组索引种子值(PISeed)生成加密密钥(EK)的示范流程图；

[0018] 图8是本发明实施例的利用具有私有密钥的PI管理器生成加密密钥(EK)的示范方框图，其中相应公用密钥被分配给用户设备。

具体实施方式

[0019] 单词“示范”这里是指“用作实例、示例或例子”。这里作为“示范”描述的任何实施例不一定被解释为比其它实施例更佳或更优。该详细说明中描述的所有实施例是示范实施例，用来使本领域熟练技术人员能够制造或使用本发明，而不是用来限制本发明的范围，本发明的范围由权利要求所定义。

[0020] 移动台也称作用户设备 (UE)，它可以与一个或多个基站通信。移动台经由一个或多个基站，向基站控制器或者这里所述的广播多播服务 (BCMCS) 控制器（在 3GPP 中还称之为多播广播多媒体系统 (MBMS) 控制器）发射和接收数据分组。基站和基站控制器是所谓接入网 (AN) 的网络的部分。基站和移动台是所谓无线接入网 (RAN) 的网络的部分。无线接入网在多个移动台之间传递数据分组。无线接入网可以进一步连接附加的网络，比如验证、授权和计费 (AAA) 服务器或者互联网，例如可以经由基站控制器或 BCMCS 控制器在每个移动台与这样的外网之间传递数据分组。

[0021] BCMCS 控制器经由短期密钥管理器 (SK 管理器) 传递数据。SK 管理器确定种子值，其可以是随机数、序号、时间戳 (time-stamp)、或者便于执行的其它变换值。一旦 SK 管理器确定种子值 (SKSeed)，它就把消息验证码 (MAC) 添加到种子值上。消息验证码 (MAC) 是数字标识符，并且像数字签名那样工作以确认种子值的源。可以使用公知的散列函数如 SHA-1 或 MD-5 创建 MAC，或者例如可以通过公知散列函数的变型来生成 MAC。散列函数把广播接入密钥 (BAK)（或 BAK 的推导）用作密钥以从种子值算出 MAC。由于只有广播网和广播网的用户具有广播接入密钥 (BAK)，因此 BAK（或者 BAK 的推导）被用作网络与用户之间的共享秘密。

[0022] 移动台（用户设备 (US)）可以是包括移动电话手机（称之为移动设备 (ME)）和存储器模块的移动电话，所述存储器模块比如是物理安全集成电路卡或者智能卡（称之为用户识别模块 (UIM) 或者通用集成电路卡 (UICC)），它可以是移动的或者被永久地附到移动设备 ME 上。在广播多播业务 (BCMCS) 中，用户设备的存储器模块装备有广播接入密钥 (BAK)。

[0023] 图 1 是图示本发明一个实施例的在广播多播通信服务 (BCMCS) 中提供已验证询问的无线通信系统 100 的示范性方框图。无线通信系统 100 包括多个用户设备 (UE) 102，这些设备经由无线通信链路与至少一个基站 (BS) 112 通信。在反向链路上执行从用户设备 102 到基站 112 的通信，在无线通信链路的前向链路上执行从基站 112 到用户设备 102 的通信。尽管图中只图示了一个基站 112，但是这仅仅处于简化图示本发明的目的。因此，无线通信系统 100 可以包括若干个地理分布的基站 112，以便当用户设备 102 穿过无线通信系统 100 时，为其提供连续通信覆盖。无线电接入网 116 通过基站 112 向无线通信链路上的用户设备 102 发射无线电信号，并从该用户设备 102 接收无线电信号。无线电接入网 116 或者被向用户设备 102 提供预约服务的无线电信公司所拥有，或者可以是被当用户设备 102 正在漫游时向用户设备 102 提供服务的另一个电信公司所拥有的被访问的网络。

[0024] 用户设备 102 可以采取能够从基站 102 接收信息的任何装置的形式，包括个人数字助理 (PDA)、无线电话、具有无线能力的便携式计算机、无线调制解调器、或者任何其它有无线能力的装置。用户设备 102 包括移动设备 (ME) 110，它经由无线通信链路提供与基站 112 的通信，即各种其它功能之一。用户设备 102 还包括存储器模块 (MM) 108（称之为用户标识模块 (UIM) 或通用集成电路卡 (UICC)）。MM108 可以是附加到移动设备 110 的可移动

存储器模块，或者是移动设备 110 的固定部分。随着详细说明的进行，将会进一步理解存储器模块 108 的功能。

[0025] 根据一个实施例，无线通信系统 100 利用广播多播服务 (BCMCS) 对在无线通信系统 100 内通信的用户设备 102 的预定组进行点对多点的数据分组传输。在一个实施例中，数据分组提供内容，例如新闻、电影、体育事件等，它们从基站 112 经由无线通信链路传送给用户设备 102。人们将会明白，传送给用户设备 102 的特定类型的内容可以包括多媒体数据的广泛组合（例如，文本、音频、图片、流、视频等），因而不一定局限于上述实例。

[0026] 无线通信系统 100 还包括归属服务网 114，它由向用户设备 102 的用户提供预约服务的无线电信公司所拥有，并且可以或者不可以由与无线电接入网 116 相同的电信公司所拥有（这取决于用户设备 102 是否正漫游在电信公司的服务区域之外）。归属服务网 114 包括广播多播服务 (BCMCS) 控制器 101、短期密钥 SK 管理器 106、归属用户服务器 (HSS) 104。通信链路 118 提供把信息承载信号从 BCMCS 控制器 101 传送到 SK 管理器 106 的数据路径。通信链路 120 提供从 SK 管理器 106 到基站 112 的数据路径，该基站 112 向多个用户设备 102 进行广播 / 多播。

[0027] 内容供应商 122 提供广播 / 多播给用户设备 102 的内容。内容供应商 122 可以是第三方内容源，他既不由归属网电信公司所拥有也不由服务网电信公司所拥有。归属服务网 114 中的归属用户服务器 104 可以包括保持移动电话预约和收集广播多播服务的帐单数据的数据库。在所示实施例中，归属服务网 114 还包括广播多播服务 (BCMCS) 控制器 101，它调度来自内容供应商 122 的内容的广播 / 多播，并执行广播 - 多播服务的至少某些安全功能。无线电接入网 116 经由专用信道把内容发送给单个用户；如果需要服务的用户的数量不能证明向覆盖区中的所有用户广播服务有道理，则经由专用信道向多个用户多播内容；或者如果需要服务的用户数量超过预定阈值，则向覆盖区中的所有用户广播内容。

[0028] 广播 - 多播服务 (BCMCS)（或多播 - 广播 - 多媒体系统 (MBMS)）内容观看是基于密钥层级的。BCMCS 或者 MBMS 可以使用相同的密钥层级，该术语的使用取决于使用它们的语境（例如，当涉及 3GPP 网中广播服务时，经常使用 MBMS）。内容观看也许需要帐单或者管理发布的监视，比如“成人”服务要求内容供应商确保观看者被准许观看“成人”服务。例如，“成人”服务的内容观看者可能被要求验证，它们是管理者确定的观看这种内容的最低年龄。密钥是与加密算法一同工作以产生特定密文的值。密钥通常是非常大的数字并且按比特测量。为了在特定时间解密广播内容，用户设备的 ME 110 应当知道当前解密密钥。为了避免未授权访问或服务盗用，解密密钥应当频繁改变，比如每分钟改变一次。这些解密密钥被称之为短期密钥 (SK)，并用来解密比较短时间量的广播内容，所以可以假设 SK 对于用户具有某些数额的固有币值 (intrinsic monetary value)。

[0029] 在一个实施例中，在广播 - 多播系统中，经过几个级别的加密和解密，来加密和解密多媒体事件的内容，以提供至少某些级别的保证，即保证未授权用户将不能解密数据及观看多媒体事件。通信链路 118 被 BCMCS 控制器 101 用来把广播接入密钥 BAK 传送给 SK 管理器 106。SK 管理器 106 确定一个值 SKSeed，并添加由 SKSeed 和共享秘密 BAK 形成的消息验证码 (MAC)。SKSeed 可以是随机数、序号、时间戳或其它可变值。然后经由无线电接入网 116 把询问 SKSeed || MAC 发送给用户设备 102。一旦在存储器模块 108 中收到该询问，用户设备 102 就首先从 SKSeed 和 BAK 中算出 XMAC。XMAC 是使用作为密钥的 BAK 或者 BAK 的推

导,通过运行散列函数导出的种子值的消息验证码。存储器模块 108 随后将 XMAC 与已收到的 MAC 进行比较。如果 XMAC 的已计算值是与已接收的 MAC 的值相同的值,则存储器模块生成 SK 并把 SK 发送给 ME。因而,如果在保护 BAK(或者源自 BAK 的密钥)的足够安全的硬件(比如智能卡)中执行这些功能,则基本上避免了未授权用户用 SKSeed 流的全部知识预先算出短期 SK。

[0030] 图 2 是在用户设备 102 处使用随机数生成短期密钥 SK 的示范性方框图。存储器模块 108 中的函数(如散列函数)用从 ME 110 输入的任何随机数 201 计算短期密钥 SK。所有广播用户具有设置在存储器模块 108 中的广播接入密钥 BAK。由于短期密钥 SK 202 是随机数 201 和 BAK 的函数,因此任何随机数输入将生成短期密钥(SK)202。因而在此情况下,具有设置在存储器模块 108 中的 BAK 的用户可以把任何范围的随机数 201 输入给存储器模块 108,并生成短期密钥 SK202 的值。用户随后可以例如在互联网上公布或分配短期密钥 SK 202 的这些值,未授权用户可以使用这些 SK 值观看内容。

[0031] 图 3 是在用户设备 102 上使用具有添加在其上的消息验证码(MAC)304 的种子值(SKSeed)生成短期密钥 SK 的示范性方框图。BCMCS 用户的用户设备 102 具有存储器模块 108,其内设有广播接入密钥 BAK。在该实施例中,存储器模块 108 还包含散列函数。散列函数可以是公知的散列函数如 SHA-1 或者 MD-5,或者公知散列函数的变型。存储器模块 108 通过使用作为密钥的 BAK(或者 BAK 的推导)运行散列函数,计算种子值 SKSeed 的生成的消息验证码,XMAC。存储器模块 108 随后将计算的 XMAC 与添加的 MAC 进行比较。如果 XMAC 和 MAC 是相同的值,则存储器模块 108 生成短期(SK)202 密钥,并且把 SK 202 发送给移动台设备(ME)110。ME 110 现在可以观看内容。在此情况下,不确认 SK 的源,就不能生成 SK。因此,与图 2 的方法不同,未授权用户不能得到 SK 值,因为只有通过确认 SK 的源才能生成 SK。图 4 示出了根据本发明一个实施例生成短期密钥 SK,以用于在用户设备 102 解密已接收内容的方法。短期密钥 SK 生成处理 400 开始于方框 402,在该方框中,用户设备 102 的存储器模块 108 接收添加有消息验证码的种子值 SKSeed。在方框 404,存储器模块 108 通过使用作为密钥的 BAK(或 BAK 的推导)运行散列函数,计算种子值(SKSeed)的消息验证码(XMAC)。记住,BAK 被设置在存储器模块(108)中,种子值可以由 SK 管理器或者 BCMCS 控制器生成。散列函数驻留在存储器模块中。在方框 406 中,存储器模块 108 将已计算的 XMAC 与已接收的 MAC 进行比较。存储器模块 108 随后在方框 408 中确定 XMAC 和 MAC 的值是否相等。如果值相等,则存储器模块 108 得知值得信赖的种子值 SKSeed 的源,因为它具有共享秘密 BAK。一旦存储器模块 108 确定 SKSeed 的源是值得信赖的,就生成短期密钥 SK,并把 SK 发送给 ME 110(方框 412)。ME 108 现在可以使用短期密钥 SK 解密已接收内容,以准许用户设备 102 的用户成功地观看内容。然而,如果在方框 408,XMAC 的计算值和 MAC 的已接收值不相等,则丢弃 SKSeed 并在方框 402 中再一次开始处理。

[0032] 在图 5 所示的另一个实施例中,SK 管理器 106 确定种子值(SKSeed)并添加被存储器模块 108 检验的数字签名。在该特定实施例中,SK 管理器 106 具有私有密钥 504,存储器模块 108 具有相应的公共密钥 506。该公共方案可以利用公知的数字签名,比如 Rivest-Shamir-Adleman(RSA)、Digital Signature Algorithm(数字签名算法)、DSA、EllipticCurve(椭圆曲线)DSA、或其它公知签名。SK 管理器 106 确定种子值(SKSeed)并添加由 SK 管理器 106 中的私有密钥 504 形成的数字签名。然后把询问 SKSeed || 数字签名

发送给存储器模块 108。ME 110 经由基站 112 接收该询问，并把 SKSeed 和数字签名 508 传送到用户设备 102 的存储器模块 108。通过使用 RSA、数字签名算法 DSA、椭圆曲线 DSA 或其它公知或未知签名方案，检验 SK 管理器经由基站 112 发送然后经由 ME110 到存储器模块 108 的签名，存储器模块 108 使用公用密钥。在存储器模块 108 中，公用密钥 506 用来验证数字签名，这是通过使用公用密钥 506 和添加的私有密钥 504 实现的。如果存储器模块 108 确定数字签名是 SK 管理器 106 建立的，则存储器模块 108 生成短期密钥 SK 202，并将 SK 202 发送给 ME110。一旦成功地生成短期密钥 SK 202，则 ME 110 准许用户观看已接收的信息内容。如果存储器模块 108 确定数字签名也许不是由 SK 管理器 106 建立的，则存储器模块 108 丢弃该签名，并等候下一个数字签名，ME 110 不能确定或者公布与该 SKSeed 对应的 SK 值。这避免了 SK 的预先计算，并有助于保护信息内容使之免于未授权的访问。

[0033] 在另一个实施例中，相同方法和设备用作安全实时传输协议 (SRTP) 的增强。2003 年 12 月届满的参考 SRTP 草案 09 公开了该协议。主密钥 (MK) 像共享秘密 BAK 一样来对待。每个 MK 具有一个索引，类似于 BAK 中的索引。该索引标识特定内容。MK 驻留在存储器模块 108 中，并且当与分组索引一起使用时，生成短期密钥 (SK)。SRTP 中的分组索引通常是序号，并且在该语境中可以认为类似 SKSeed，可以采用随机数、序号、时间戳或者其它变化值。MK 和分组索引用来生成 SRTP 加密密钥 (EK)。该加密密钥类似 SK，用来观看或访问内容。因而，分组索引必需是安全的，以防止未授权访问或内容偷盗。分组索引可以被保护，其保护方式与种子值 (SKSeed) 添加消息验证码 (MAC) 以用来保护 SK 的方式相同。通过把消息验证码 (MAC) 添加到分组索引上，存储器模块 108 将知道分组索引是否来自预期信任的源。存储器模块 108 以用来生成 SK 的相同方式进行该处理。像生成加密密钥一样，SRTP 指定可能以模拟方式从主密钥 MK 生成的其它密钥来执行其它功能，这些功能包括上述的消息验证和对加密密钥的安全增强，它同样适用于如此生成的其它密钥。

[0034] 图 6 是使用具有附加其上的消息验证码 (MAC) 的分组索引值 (PI) 602 生成加密密钥 (EK) 的示范性方框图。任何广播用户的用户设备 (UE) 102 具有设有 MK 的存储器模块 108。在该实施例中，存储器模块 108 还包含散列函数。散列函数可以是公知的散列函数，比如 SHA-1 或 MD-5 或者公知散列函数的变型。存储器模块 108 通过使用作为密钥的 MK 或者 MK 的推导运行散列函数，来计算分组索引值 PI 的 XMAC。存储器模块 108 随后将计算的 XMAC 与附加的 MAC 进行比较。如果 XMAC 和 MAC 是相同值，则存储器模块 108 生成加密密钥 (EK) 604 并把 EK 604 发送给移动设备 (ME) 110。一旦成功地生成 EK 604，ME 110 通过使用 EK 604 解密已接收的加密内容，就可以观看内容。在此情况下，不确认 EK 604 的源，就不能生成 EK 604。因而，该情况防止未授权用户观看或访问信息内容。

[0035] 图 7 图示了 SRTP 加密密钥生成处理 700，其中存储器模块 108 接收附加有消息验证码的分组索引值 PI (方框 702)。在方框 704，存储器模块 108 通过使用作为密钥的 MK 或 MK 的推导运行散列函数，算出分组索引值 (PI) 的消息验证码 (XMAC)。所有广播用户都具有设置在存储器模块 108 中的 MK。在方框 706 中，存储器模块 108 将计算的 XMAC 与已接收的 MAC 进行比较。存储器模块 108 在方框 708 判断 XMAC 和 MAC 的值是否相等。如果这两个值相等，则存储器模块 108 知道分组索引值 (PI) 的源是可信赖的，因为它具有共享秘密 MK。一旦存储器模块 108 确定 PI 的源是可信赖的，则它生成加密密钥 (EK) 604 并向 ME 110 发射加密密钥 EK 604 (方框 712)。一旦 EK 604 成功生成，ME 110 就可以观看内容。如果

XMAC 和 MAC 不相等 (方框 708), 则丢弃 PI, 并在方框 702 重新开始处理。

[0036] 在另一个实施例中, 通过使用附有数字签名的分组索引, 可以保护分组索引。在该实施例中, 如图 8 所示, 分组索引 (PI) 管理器 802 确定分组索引值 (PI), 并附加将被存储器模块 108 确认的数字签名。在该实施例中, PI 管理器 802 具有私有密钥 504, 存储器 108 具有相应的公用密钥 506。该公用方法可以利用公知的数字签名, 比如 Rivest-Shamir-Adleman (RSA)、数字签名算法、DSA、椭圆曲线 DSA 或者其它公知签名。PI 管理器 802 确定分组索引值 (PI) 并在 PI 管理器 802 中附加由私有密钥 504 形成的数字签名。然后发射询问 $PI \parallel$ 数字签名。ME 110 经由基站 112 接收该询问, 并且将 PI 和数字签名 804 转给存储器模块 108。存储器模块 108 通过使用 RSA、数字签名算法 DSA、椭圆曲线 DSA 或者其它公知或未知签名方案检验 PI 管理器 802 经由基站 112 发射的通过 ME110 到达存储器模块 108 的签名, 来使用公用密钥。在存储器模块 108 中, 公用密钥 506 检验数字签名, 这是通过使用公用密钥 506 和附加的私有密钥 504 实现的。如果存储器模块 108 确定数字签名是由 PI 管理器 802 建立, 则存储器模块 108 生成加密密钥 (EK) 604, 并把 EK 604 发射给 ME 110。ME 110 一旦成功接收到 EK 604, 就可以马上观看信息内容。如果存储器模块 108 确定数字签名也许不是 PI 管理器 802 建立的, 则存储器模块 108 丢弃该签名并等候下一个数字签名, ME 110 不能确定或公布与该 PI 对应的 EK604 值。这避免了分组索引的预算, 并有助于保护信息内容免于未授权访问。

[0037] 涉及 SRTP 的实施例还提供了避免验证和 salting 密钥的未授权生成的附加安全性。这类似于在 BCMCS/MBMS 中防止 SK 的预算。此外, 在 SRTP 中, 一旦服务供应商把相同的主密钥 (MK) 配置到多个终端用户的安全存储器模块 108 上, 终端用户可以伪装成服务供应商。这是因为在安全存储器模块 108 中设有 MK 的任何终端用户可以使用安全存储器模块 108 加密和增加对数据的验证。上述实施例避免了这种情况, 因为 PI 管理器 802 通过使用 MAC 或数字签名, 确保加密密钥生成仅仅可以发生在分组索引的源被验证为可信赖源的时候。

[0038] 本领域数量技术人员将会明白, 可以使用各种不同技术来代表信息和信息。例如, 可以用电压、电流、电磁波、磁场或者粒子、光场或粒子、或者其任何组合表示上述整个说明涉及的数据、指令、命令、信息、信号、比特、符号和码片。

[0039] 那些熟练技术人员将会进一步明白, 结合这里公开的实施例描述的各种说明性逻辑块、模块、电路和算法步骤可以被实施为电子硬件、计算机软件或者其组合。为了清楚地说明硬件和软件的可互换性, 各种示范性部件、块、模块、电路和步骤在上文中通常根据它们的功能描述。不管这种功能被实施为硬件还是软件, 都取决于特定的应用, 并且设计约束影响整个系统。熟练的技工可以为每个特定应用, 以不同方式实施所述功能, 但是这种实施决定应当不被解释为造成背离本发明的范围。

[0040] 结合本发明实施例描述的各种说明性逻辑块、模块和电路可以用通用处理器、数字信号处理器 (DSP)、专用集成电路 (ASIC)、现场可编程门阵列 (FPGA) 或者其它可编程逻辑装置、分立门电路或者晶体管逻辑、分立硬件部件、或者设计执行所述功能的任何组合来实施或执行。通用处理器可以是微处理器, 但是在任何一个替代中, 处理器可以是任何传统的处理器、控制器、微处理器或者状态机。处理器还可以被实施为计算装置的组合, 例如 DSP 和微处理器的组合、多个微处理器、与 DSP 内核结合的一个或多个微处理器、或者任何其它的

这种配置。

[0041] 结合本发明实施例所述的方法或算法的步骤可以被直接并入硬件中、由处理器运行的软件模块中、或者两者的组合。软件模块可以驻留在 RAM 存储器、闪存、ROM 存储器、EEPROM 存储器、寄存器、硬盘、活动盘、CD-ROM、或者本领域已知的任何其它形式的存储媒介。示范性存储媒介连接处理器，使该处理器可以从存储媒介中读取信息，并把信息写到存储媒介中。在替代中，存储媒介可以被集成到处理器上。处理器和存储媒介可以置于 ASIC 中。ASIC 可以置于用户终端中。在替代中，处理器和存储媒介可以作为分立部件置于用户终端中。

[0042] 所述实施例的上述说明用来使本领域熟练技术人员能够制造或者使用本发明。这些实施例的各种修改对于本领域熟练技术人员是显而易见的，并且这里定义的基本原理可以应用于其它实施例，而又不背离帮倒忙锁网精神和范围。因此，本发明不打算局限于所示的实施例，而是与遵从本发明的原理和新颖性特点的最宽范围相一致。

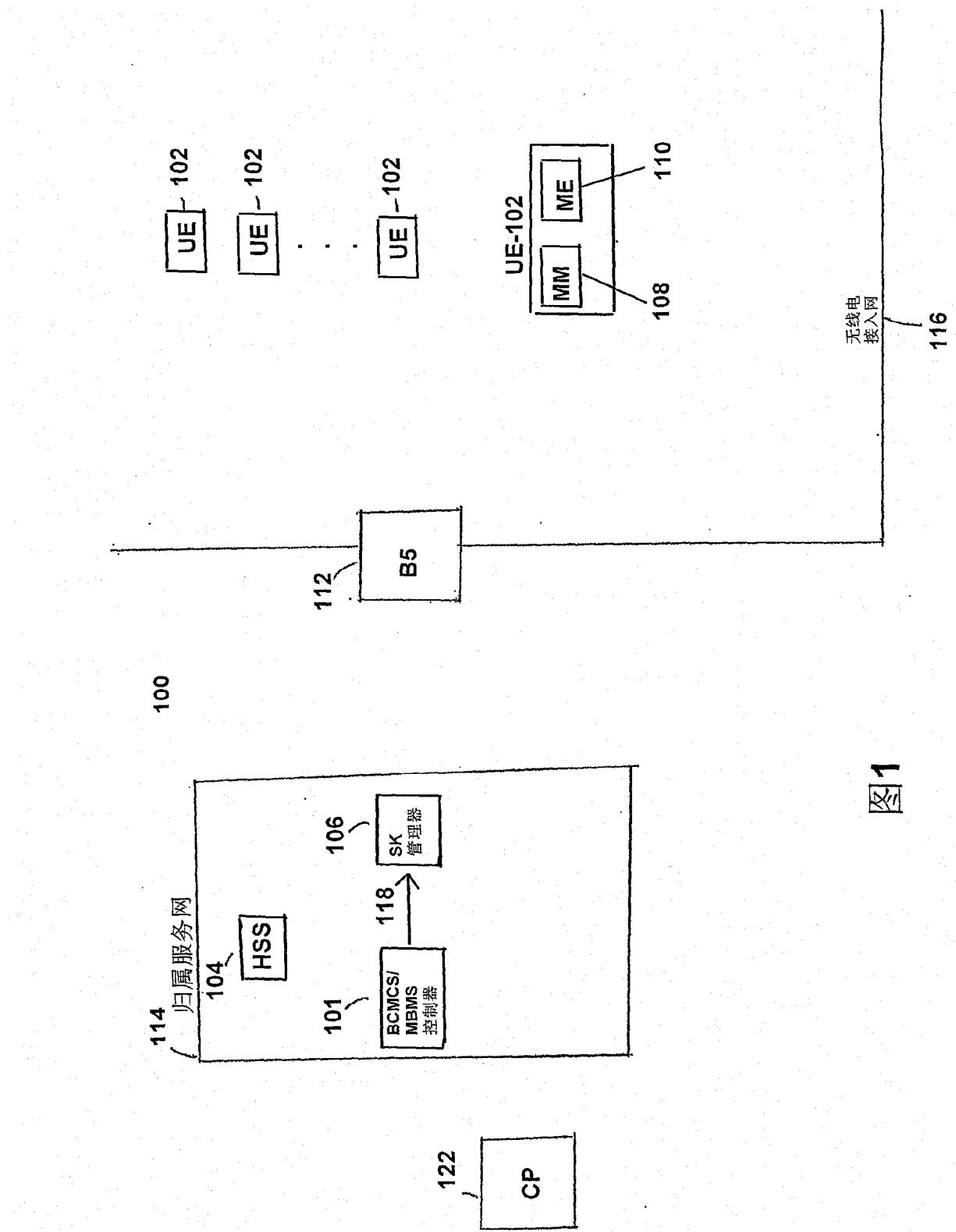


图1

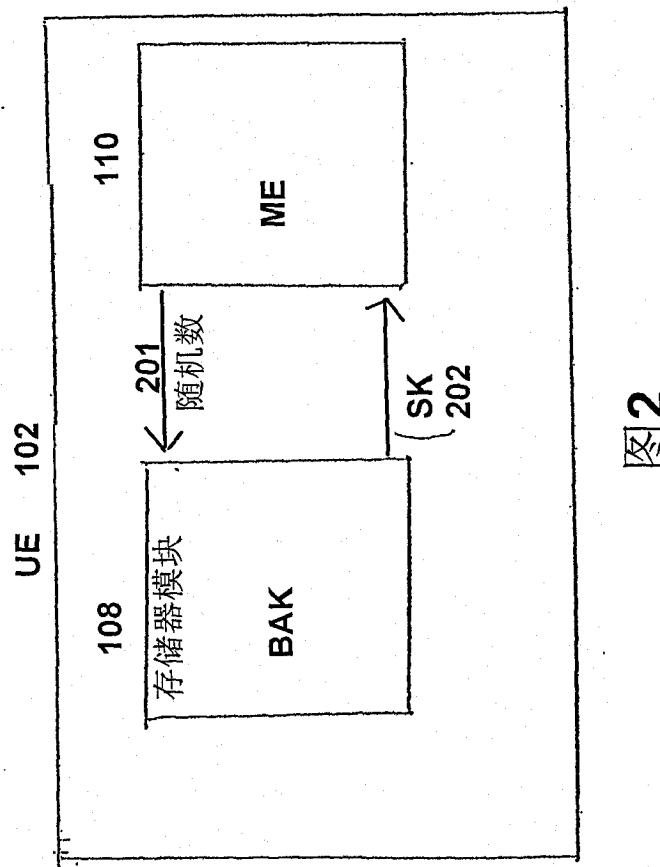


图2

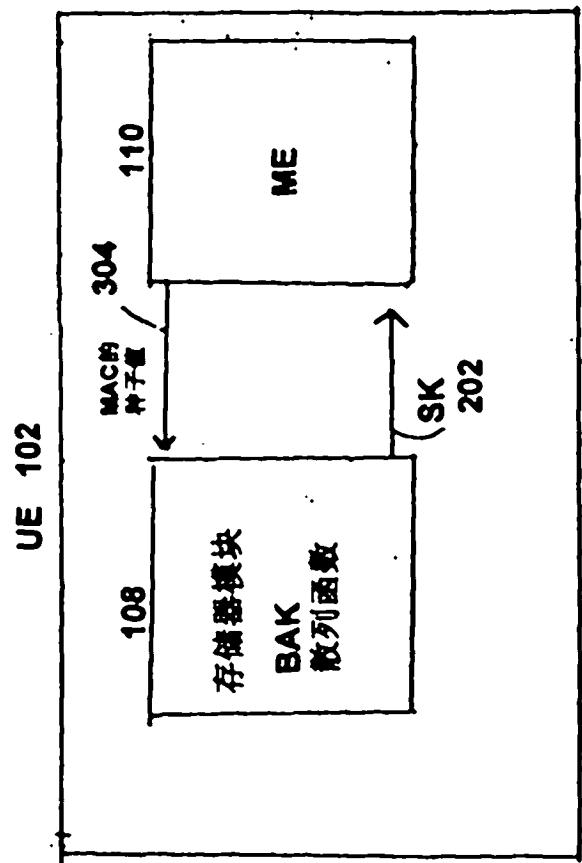


图3

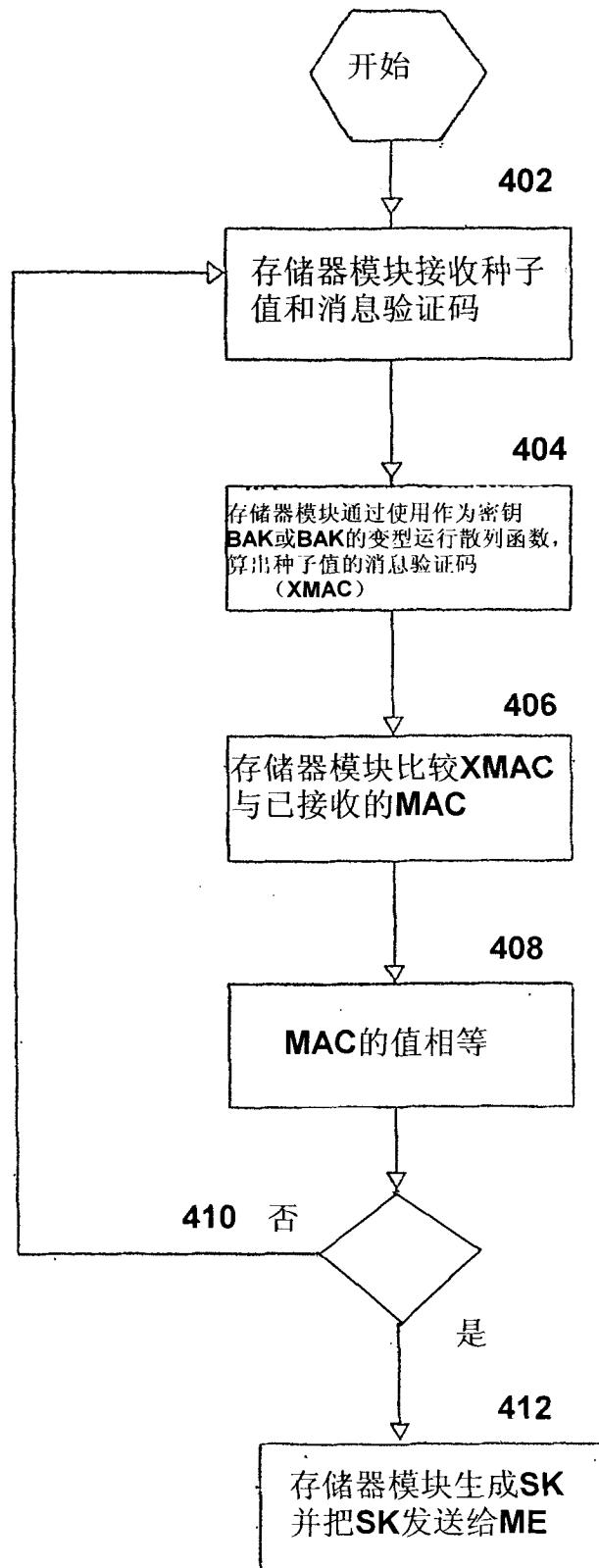


图 4

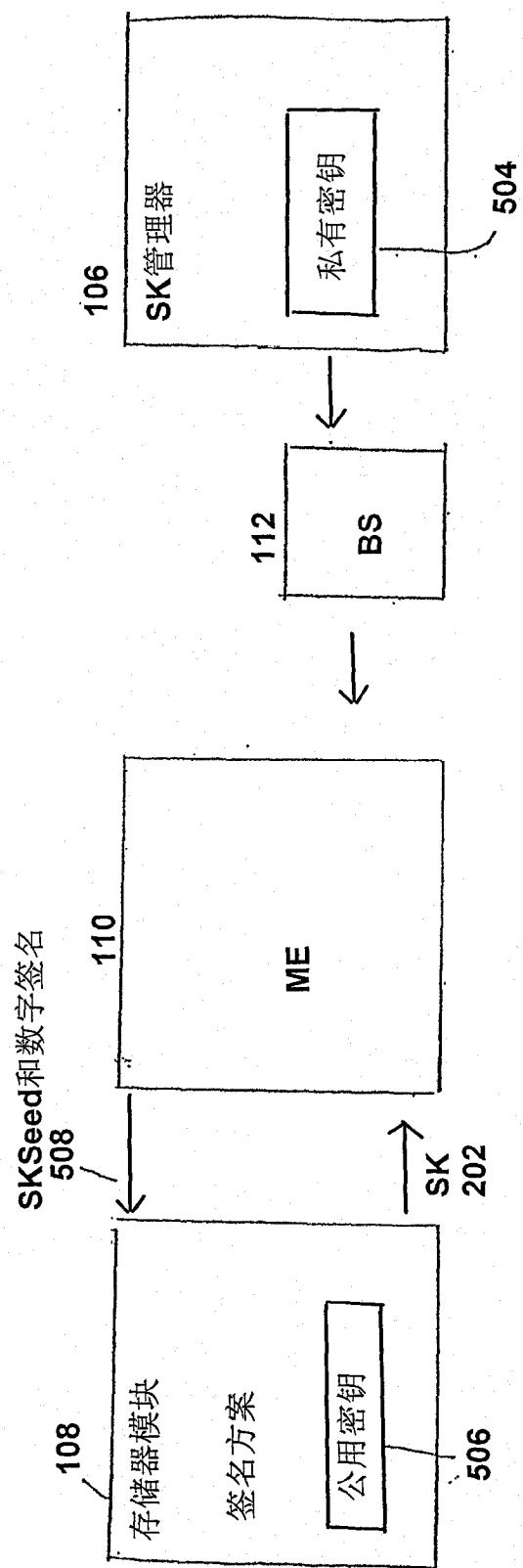


图5

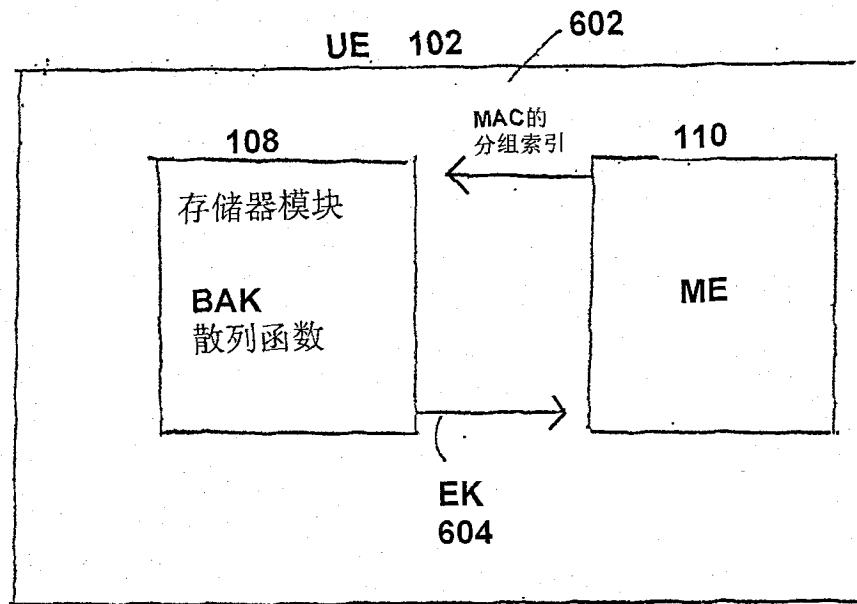


图6

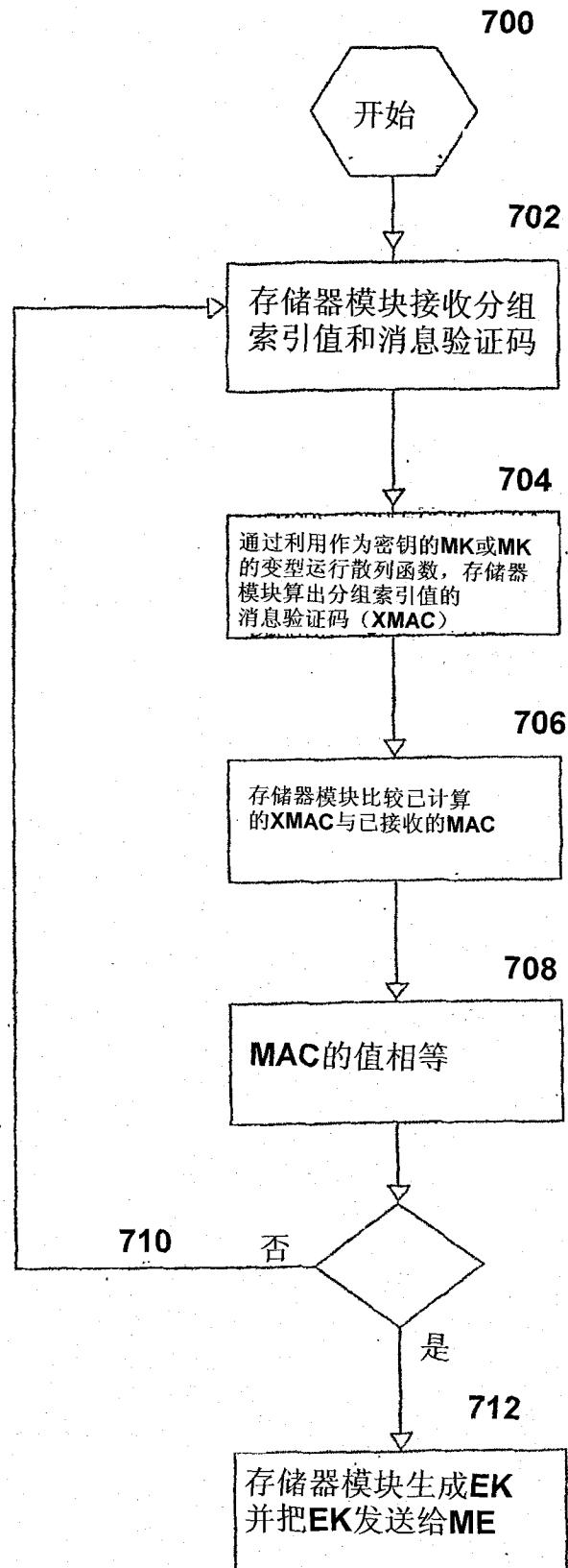


图 7

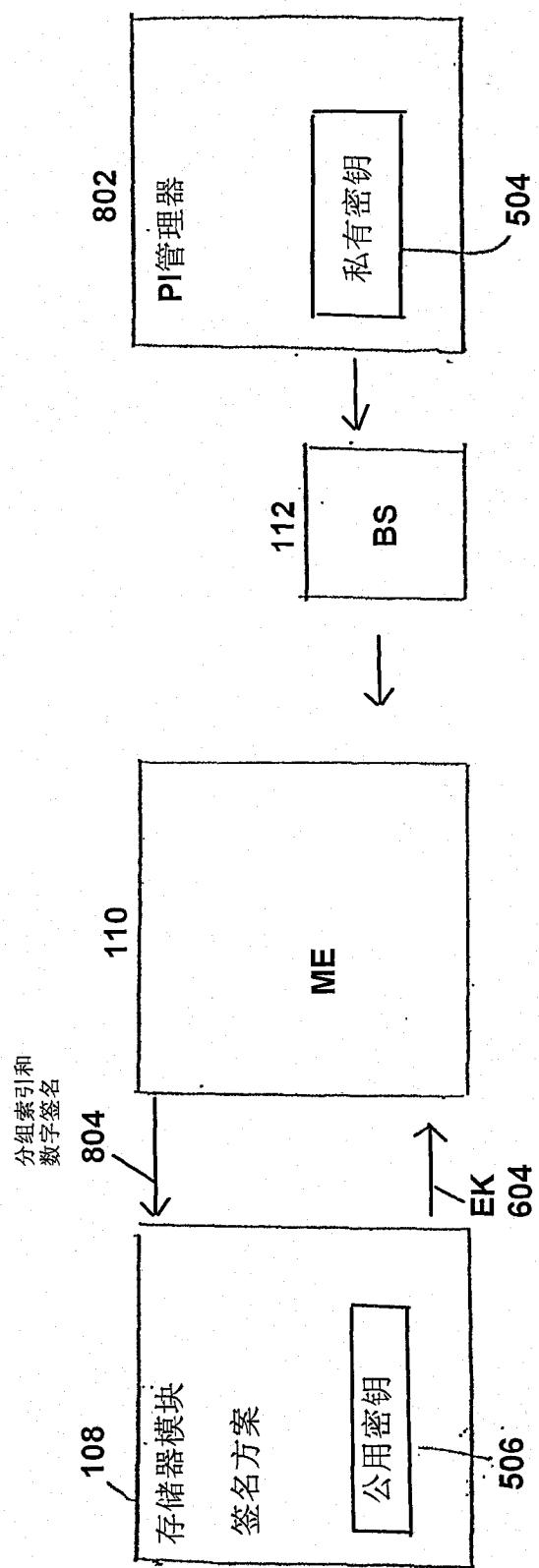


图8